ITS Customer Driven Technology
Information Technology Services

Standards and Architecture Document for State Interoperability: 802.11b Wireless environment with port level security (IEEE 802.1x)

Version 1.2
January 29, 2004
ITS Wireless Product Team

Document Information

This document was created by the ITS 802.11 product team to describe the architecture and technical standards used as the foundation for the ITS Wireless LAN product.

Change Date	Type of Change	Change(s) Made	Reason for Change
7/22/03	First Draft		
11/19/03	Second Draft, 1b	Miscellaneous additions	Reviewer comments
12/2/03	Third Draft, 1c	Miscellaneous changes	Reviewer comments
12/8/03	4th Draft, 1d	Miscellaneous changes	Reviewer comments
12/9/03	5th Draft, 1e	Nancy's edits	Reviewer comments
1/28/04	6th Draft, 1.1	Rick's additions: table, glossary and definitions. Team edits.	Reviewer comments
1/28/04	7th Draft, 1.2	Nancy's edits	Reviewer comments

Introduction and Purpose

This document describes the architecture and technical standards for the ITS Wireless LAN Product. Wireless LANs implemented using these standards will ensure secure wireless access to State IT resources and provide interoperability for state employees who travel between state facilities and want wireless data access in this mobile mode.

These standards are intended for use by: 1) ITS to implement Wireless LANs for customer agencies; and, 2) by agency customers who want to implement their own Wireless LAN and meet state interoperability and security standards.

The ITS Wireless LAN architecture and standards were developed based on the following requirements:

1. Enterprise-class design.
2. Secure access to State IT resources.
3. Interoperability for authorized users in state facilities implemented in accordance with the standard.
4. 802.1x compliant.
5. Authentication, authorization, and accounting using the Utah Master Directory (UMD).
6. Elimination of the use of pre-shared key authentication.
7. Privacy of user credentials and data.
8. End-user ease of use.

The components of the ITS Wireless LAN architecture and standards included in this document are:

- Access points
- RADIUS Services
- Authentication directory
- Wireless cards
- EAP supplicant

Future versions of the ITS Wireless LAN product and standards will be enhanced for the following items, and others as submitted by customers:

- Testing and adding additional wireless access points to the standard.
- Testing and adding additional wireless cards to the standard.
- Testing and adding PDAs and other devices to the standard.
- Additional platforms such as Linux and Mac OSX
- Enhancements as the technology evolves and matures.

Architecture Overview

The overall architecture and standard is based on 802.1x specification, a subset of the IEEE 802 standards. This defines controlling access to physical or virtual MAC (Media Access Controls) ports based on authentication and authorization using a MAC layer frame carrying EAP—Extensible Authentication Protocol over LAN authentication data. EAP is an extension of the Point-to-Point Protocol.

Protecting user credentials and authenticating the server using a server certificate over Transport Layer Security (TLS) is referred to as Protected EAP (PEAP), also called EAP-GTC—Generic Token Card, or Cisco EAP. The Internet Engineering Task Force (IETF[1]) is considering Multiple EAP standards, including EAP-TLS—Microsoft, EAP-GTC—Cisco and EAP-TTLS—Funk Software. The PEAP Authentication process is illustrated in Figure 1.

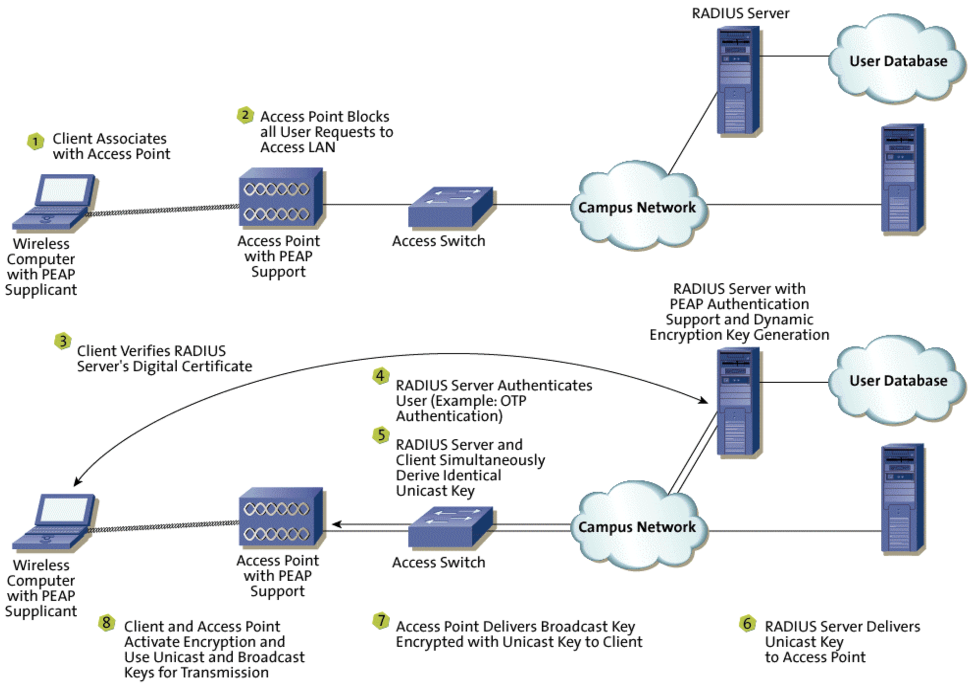
RADIUS Server
User Database
1 Client Associates with Access Point
2 Access Point Blocks all User Requests to Access LAN
Wireless Computer with PEAP Supplicant
Access Point with PEAP Support
Access Switch
Campus Network
RADIUS Server with PEAP Authentication Support and Dynamic Encryption Key Generation
3 Client Verifies RADIUS Server's Digital Certificate
4 RADIUS Server Authenticates User (Example: OTP Authentication)
5 RADIUS Server and Client Simultaneously Derive Identical Unicast Key
User Database
Campus Network
Access Switch
Wireless Computer with PEAP Supplicant
Access Point with PEAP Support
8 Client and Access Point Activate Encryption and Use Unicast and Broadcast Keys for Transmission
7 Access Point Delivers Broadcast Key Encrypted with Unicast Key to Client
6 RADIUS Server Delivers Unicast Key to Access Point

Figure 1: PEAP Authentication Process

The ITS PEAP implementation will be EAP-GTC, or Cisco PEAP. This approach keeps costs to down because the product is already owned and supported by ITS. This implementation of the PEAP standard protects the Wireless LAN as the Access Points will not permit a connection until the user is authenticated. As well, it protects user credentials over a TLS tunnel. Moreover, this approach prevents man-in-the-middle attacks by using dynamic WEP keys derived from unique session information. This Cisco EAP Authentication process is illustrated in Figure 2.

[1] Internet Engineering Task Force. There are two implementations of PEAP, as proposed by Cisco Systems, Inc. and by Microsoft. Protected EAP or EAP-GTC (Generic Token Card) as proposed by Cisco will authenticate against multiple authentication databases. PEAP as proposed by Microsoft requires authentication databases that use MS-CHAP.

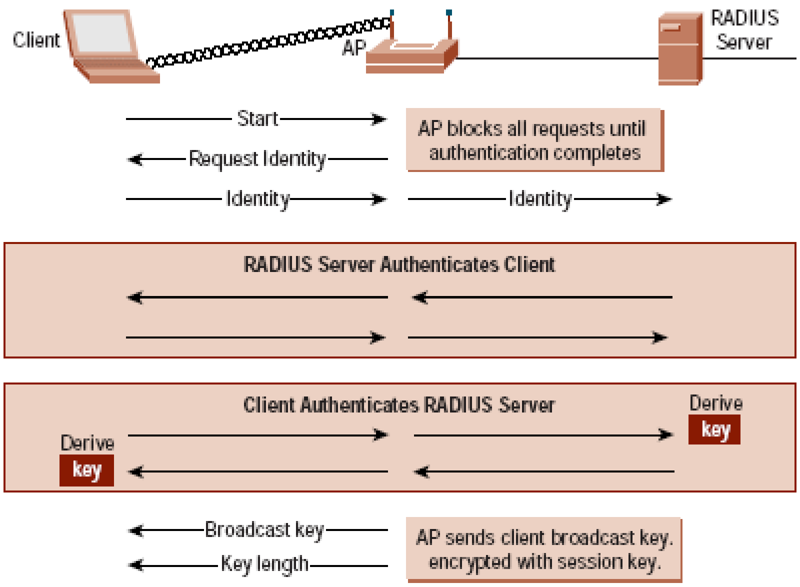
Client
AP
RADIUS Server
Start
Request Identity
Identity
AP blocks all requests until authentication completes
Identity
RADIUS Server Authenticates Client
Client Authenticates RADIUS Server
Derive key
Derive key
Broadcast key
Key length
AP sends client broadcast key, encrypted with session key.

Figure 2: Cisco EAP Authentication

The ITS Wireless LAN product architecture and standards include the following components:

Component	***Standard***	**Item**
Access Point	802.1x and WPA (Wi-Fi Protected Access)	Cisco model 1230
RADIUS Server		Cisco Secure ACS (Access Control Server), version 3.1 or greater
Authentication Directory	LDAP	Utah Master Directory (UMD)
802.11 Client (Wireless Cards)	802.1x and WPA	• ITS has tested: o Enterasys RoamAbout 802.11b o 3Com 802.11 A, B, G with Xjack antenna o Cisco Aironet 350 o Intel Centrino built-in 802.11b • Any PEAP capable 802.1x-compliant device should operate. However some manufacturers include proprietary features that cause problems.
EAP Supplicant	802.1x	Two options: • Funk Software Odyssey, version 2.2 or greater. This option is strongly recommended. • Cisco Aironet Client Utility (ACU), version 5.0 or greater. This option is functional, but not as feature rich.
Device Platforms		• Windows versions 98, 2000 and XP. • Pocket PC (Windows CE 2002) • Cisco ACU – additional platforms available (www.cisco.com)

Architecture Component Detail

Access Point (WAP)

As this solution is deployed statewide, a consistent SSID will allow for uniform, authenticated access wherever implemented within State facilities.

While other vendors comply with this standard, ITS has tested and installed WAPs from Cisco Systems, Inc. These WAPs use the Cisco Internetworking Operating System (IOS) consistent with all the routers and many of the Ethernet switches in use on the State WAN. This allows ITS to leverage existing skills in working with these devices. In addition, using IOS, these devices can be configured to restrict access based on access control lists (ACLs).

The WAPs are configured for PEAP authentication, meaning they "challenge" the client for credentials (login id and password). The WAP then uses the RADIUS (Remote Authentication Dial-In User Service) protocol to validate the login to the WAP. The RADIUS service validates against a user database (e.g., LDAP, NDS and Win NT).

WAPs can also be configured to function in a redundant, fail-over mode for installations where high availability is required.

RADIUS Server and Authentication Directory

RADIUS is a protocol for validating authentication and authorization credentials between a networked device and a shared Authentication Server. It was originally proposed by the IETF in RFC (Request for Comment) 2138 and refined in RFC 2865.

Pursuant to the RADIUS standard, the networked device (NAS) functions as a ***client*** of the RADIUS service (operating on a RADIUS server). The NAS receives user credentials and passes them to the RADIUS server. The RADIUS server can forward these requests to external authentication sources.

For the ITS product, authentication requests will be sent over LDAP queries to the State master authentication directory UMD (Utah Master Directory). The RADIUS standard requires authentication between the NAS and the RADIUS server by using a shared secret. The shared secret is not sent over the network and user passwords are encrypted when sent between the NAS client and the RADIUS server.

Cisco Secure Access Control Services (ACS—RADIUS Server)

The Cisco ACS for RADIUS services was selected for both technical and economic reasons. ITS owns two Cisco RADIUS server licenses and interfaces with LDAP and NDS—two of the basic components of UMD. The ACS server also interfaces with the standard Cisco WAPs as well as all other Cisco hardware owned or operated by ITS. This enables RADIUS authentication to be leveraged by other services such as Dial-up, VPN, Wireless and command line administration of other networking hardware (routers and switches).

RADIUS implementations include logging of user access. These logs can be harvested for customer activity and billing information.

802.1x Client (Wireless Cards)

The term “client” refers to the user device required for accessing the Wireless LAN. This can be a wireless adapter built into a laptop or a PCMCIA card. The basic requirement for the client network adapter is complying with IEEE 802.1x.

For the initial release of the product, ITS has tested three PCMCIA wireless cards and two built-in adapters.

EAP Supplicant

One critical element of any wireless network is security. The ITS wireless architecture provides enhanced security by implementing authenticated, encrypted client access for service. Authorization and access control will rely on Protected EAP (PEAP).

Part of implementing the IEEE standard for 802.1x port-based access control requires client software for adding the EAPOL (EAP over LAN) data to the MAC header of the Ethernet frame. This software is called EAP Supplicant.

While there are PEAP solutions available from both Microsoft and Cisco, the Microsoft implementation of the PEAP standard requires MS-CHAP for communicating with the authentication directory. MS-CHAP is incompatible with both LDAP and NDS. Accordingly, the 802.1x supplicant should be capable of:

- Compliance with the Cisco implementation of PEAP (Protected Extensible Authentication Protocol).
- Compatibility with PAP (Password Authentication Protocol).
- Compatibility with Cisco Secure ACS RADIUS.
- Operating on Windows XP, 2000, 98 and Millennium Edition (at a minimum—other platforms will prove to be strategic as well).
- Pre-configurable parameters for ease of deployment.
- Supporting auto-reconnect to the Wireless LAN.
- Retaining user profile information.

ITS has tested several EAP Supplicant options and selected two that are compatible with this deployment. The two options are: Odyssey, by Funk Software (available through PC Stores vendors) and the Cisco Aironet Client Utility (ACU) that is provided “free” with the purchase of Cisco wireless cards.

It is important to note that those who have used both the Odyssey and the Cisco ACU clients recommend using the Odyssey client, which is feature rich.

Conclusion

These 802.11 Wireless LAN Architecture and Technical Standards provide for a robust, secure product that can be implemented across state facilities and meet product requirements.

Future versions of the ITS Wireless LAN product and standards will be enhanced for the following items and others as submitted by customers:

- Testing and adding additional wireless access points to the standard.
- Testing and adding additional wireless cards to the standard.
- Testing and adding PDAs and other devices to the standard.
- Additional platforms such as Linux and Mac OSX
- Enhancements as the technology evolves and matures.

Glossary

IEEE (Institute of Electrical and Electronics Engineers): IEEE is an industry organization of engineers, scientist and students involved with defining standards for computers and communications, including Ethernet specifications.

IETF (The Internet Engineering Task Force): IETF is a non-membership, open and voluntary standards organization dedicated to identifying problems and opportunities in IP data networks and proposing technical solutions to the Internet community.

ITU (International Telecommunications Union): ITU is an international organization, now part of the United Nations that sets standards for global telecommunications networks. ITU was formerly known as the CCITT, the Consultative Committee for International Telephony and Telegraphy.

LDAP (Lightweight Directory Access Protocol): LDAP is a protocol used to access a directory. LDAP is a simplified version of the DAP protocol, which is used to gain access to ITU X.500 directories.

NAS (Network Access Server): NAS is a RADIUS standard as defined by IETF RFC 2138—superseded by RFC 2865, which defines the networked device requiring authentication and authorization for use as the Network Access Server.

NDS Novell Directory Services: NDS Novell Directory Services is Novell's flagship directory service that was included in NetWare (as NDS) beginning with Version 4. It is also available for Windows NT/2000, Solaris and Linux. It is based on the X.500 directory standard and maintains a hierarchical database of information about the network resources within a global enterprise, including networks, users, subgroups, servers, volumes and printers. eDirectory users log onto the network and eDirectory determines their access rights. eDirectory also supports LDAP.

PAP (Password Authentication Protocol): PAP is the most basic control protocol for logging onto a network. A table of usernames and passwords are stored on a server. When users log on, the names and passwords are sent to the server for verification.

PEAP (Protected Extensible Authentication Protocol**):** PEAP, pronounced “peep”, is a protocol developed jointly by Microsoft, RSA Security and Cisco for transmitting authentication data, including passwords, over 802.11 wireless Ethernet networks. PEAP authenticates Wireless LAN clients using only server-side digital certificates by creating an encrypted TLS tunnel between the client and the authentication server. The tunnel then protects the subsequent user authentication exchange.

PAE (Port Authentication Entity): PAE refers to the device in the 802.1x system that prevents access until authentication and authorization are verified. The wireless access points described in this document function as PAEs.

RADIUS (Remote Authentication Dial-in User Service): RADIUS is an IETF standard defining the process for restricting access to networked devices.

RFC (Request for Comment): RFC is a document that describes the specifications for a recommended technology. RFCs are used by IETF and other standards organizations.

SSID (Service Set Identifier): SSID is a 32-character unique identifier attached to the header of packets sent over a Wireless LAN that acts as a password when a mobile device tries to connect to the network. The SSID differentiates one Wireless LAN from another. All access points and all devices attempting to connect to a specific Wireless LAN must use the same SSID. A device will not be permitted to join unless it can provide the unique SSID. Because an SSID can be sniffed in plain text from a packet it does not supply any security to the network. An SSID is also referred to as a “network name” because it is the name that identifies a wireless network.

SUPPLICANT: A Supplicant, per the IEEE 802.1x standard, is the device requesting access through the Port Authentication Entity (PAE). For purposes of this document it will also refer to the 802.1x software running on the client, enabling authentication.

TLS (Transport Layer Security): TLS is a protocol that guarantees privacy and data integrity between client-server applications communicating over the Internet.
The TLS protocol is made up of two layers:

1. *TLS Record Protocol* - layered on top of a reliable transport protocol such as TCP, it ensures that the connection is private by using symmetric data encryption and that the connection is reliable. The TLS Record Protocol is also used for encapsulation of higher level protocols such as the TLS Handshake Protocol.
2. *TLS Handshake Protocol* - allows authentication between the server and client, and the negotiation of an encryption algorithm and cryptographic keys before the application protocol transmits or receives any data.

TLS is application protocol-independent. Higher level protocols can layer on top of the TLS protocol transparently. TLS is based on Netscape’s SSL 3.0. TLS supercedes and is an extension of SSL. TLS and SSL are not interoperable.

UMD (Utah Master Directory): UMD is a flat, high-performance LDAP directory for authenticating State of Utah resources.

VLAN (Virtual Local Area Network): A VLAN is a MAC layer network of computers that behave as if they are connected to the same physical LAN although they may actually be physically located on different segments of a LAN. VLANs are configured through software rather than hardware, which makes them extremely flexible. One of the biggest advantages of VLANs is that when a computer is physically moved to another location, it can stay on the same VLAN without any hardware reconfiguration.

WAP (Wireless Access Point): A WAP is a hardware device or a computer's software that acts as a communication hub for users of a wireless device to connect to a wired LAN.

WEP (Wired Equivalent Privacy): WEP is the encryption method incorporated into the 802.11b specification to provide the wireless network with a level of security comparable to a wired LAN. Even with the 128 bit key length (WEP can use either 40 bit or 128 bit keys) WEP can be compromised using tools readily available on the Internet.

Wi-Fi (Wireless Fidelity): Wi-Fi is an interoperability certification for Wireless LAN products based on the IEEE 802.11 standard.

WLAN (Wireless Local Area Network): A WLAN, for purposes of this document, means networks based on equipment designed according to IEEE standards 802.11b, 802.11a and 802.11g.

WPA (Wi-Fi Protected Access): WPA is a standard introduced by the Wi-Fi Alliance providing for enhanced security of Wireless LANs. WPA consists of 802.1x authentication, enhanced WEP key management and improved packet integrity. The Wi-Fi Alliance is an industry committee consisting of manufactures and vendors of Wi-Fi-compliant devices.

Appendix A

ITS objectives in securing wireless traffic include:

- Confidentiality - preventing unauthorized eavesdropping.
- Data integrity - preventing the interception and manipulation of data.
- Access control - preventing users from accessing State resources—as simple as providing free Internet access and as complex as an intruder using the wireless access points as a launch for attacking other systems or compromising security to penetrate to other's data.

The following factors precipitated the selection of PEAP for the ITS Wireless LAN product:

Authentication Method	***Evaluation Criteria***			
	Level of Security	**Deployment Issues**	**Cost**	**Authentication Server**
Shared Key (e.g., WEP)	Hacking is well documented.	Keeping keys private when distributing them statewide. Requires VPN to reach wired LAN. Key administration on a large scale could become very time consuming.	LAN Admin time.	None.
EAP-TLS	User credentials are passed in clear text. Relies on 802.1x for access control to prevent "listening."	Requires PKI implementation with a certificate on each client device.	Win XP and 2000. A patch is available for NT/98. Some type of certificate server is necessary.	Cisco ACS, Free RADIUS, Funk, Meetinghouse, Microsoft.
Cisco PEAP (EAP-GTC) Essentially Cisco's implementation of EAP-TTLS	User credentials and data stream are encrypted (up to 104 bit WEP).	Configuring the Cisco ACS Server has been problematic. There is a known incompatibility with anti-virus software and with Windows patches. Requires Cisco client and card, however, Cisco has been providing other manufacturers with the software for compatibility. Can extend wired LAN.	Sunk cost, server licenses have been acquired, client comes with Aironet card.	Cisco ACS Cisco Secure Access Control Server (Cisco Se cure ACS) for Windows Server version 3.1

EAP-TTLS Meetinghouse AEGIS	User credentials and data stream are encrypted (up to 104 bit WEP).			Cisco ACS, Funk Odyssey, Meetinghouse
EAP-TTLS Funk/Odyssey	User credentials and data stream are encrypted (up to 104 bit WEP).	Requires client software on each device. Management software can facilitate bulk-load configurations. While client software is $40 per user, it provides a smooth. Can extend wired LAN.	$25-30 per client, administration time.	Funk Steel-Belted RADIUS, Cisco ACS.
Wireless Gateway (i.e. Bluesocket)	User credentials are encrypted over SSL. SSL can be susceptible to man-in-the-middle attacks. Data stream encryption requires client configuration or VPN client, otherwise all clear text.	Configuration is primarily on the gateway unless VPN or IPSec is used.	All list prices: 15 users $3500 100 users $7000 400 users $12995 Even assuming a 40% discount the metro SLC area could run $80,000. This does not include potential DPS or other agency hot spots.	Requires a wireless gateway for each IP broadcast domain (this could be expensive in global deployment) encrypts login credentials, does not encrypt wireless after authentication (unless configured for VPN termination). Requires VPN to reach wired LAN.
Open, with RADIUS authentication	User credentials are passed in clear text, nothing to prevent "listening."	Modification of router configuration, and a switch at each site.	Firewall feature set on each participating router, approx $2,000 per node.	Still requires some degree of VPN technology for internal access.
Open	No security	Minimal effort	Downtime, hacking, reputation, etc.	None